Knowing What's On Your Network

Doug Dexter

Audit Team Lead

February 26th, 2014

Cisco At a Glance

Best in the World, Best for the World

- Worldwide leader in networking
- Founded in 1984
- #13 in Best Global Brands
- $120+ billion market capitalization
- $50+ billion cash/cash equivalents
- $5.9 billion a year in R&D
- 160+ acquisitions

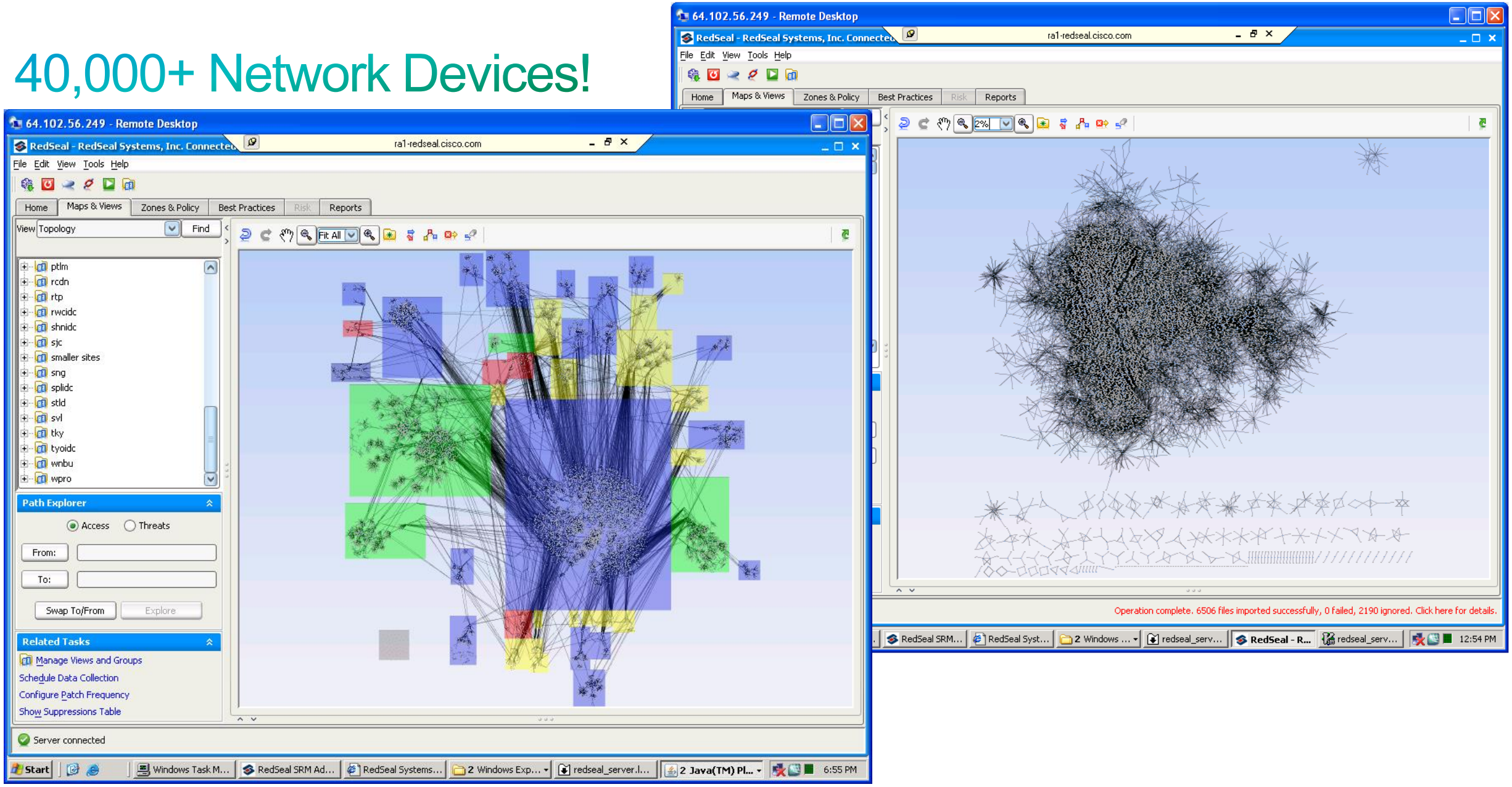
- 650+ active suppliers
- 86% of products distributed via channel
- 110,000+ employees and contractors
- 24,000+ engineers in 1800+ labs
- 14,000+ patents issued to Cisco inventors
- Global presence in 165 countries
- 165 InfoSec Staff (Blue & Red)

Cisco webex · IRONPORT · SOURCEfire · ScanSafe · STARENT NETWORKS · TANDBERG · NDS

What We're Working to Protect

- What's on the Cisco Network?
  - 1.1M public IPv4 addresses plus 1.7M private (RFC1918)
  - 125,000 Windows, 72,000 Linux, 50,000 Cisco devices, 43,000 "other"
  - 120,000 IP phones, 70,000 BYOD mobile
  - 30,000 Data Center hosts
  - 1820 labs, 100,000+ devices
  - 2400+ IT applications supporting 835 service offerings
- 16 major Internet connections, ~32 TB bandwidth used daily
- 294 partners use 547 IT extranet connections into Cisco
- 400+ cloud/ASP providers used (officially)

40,000+ Network Devices!



Cisco's Any Device Landscape

82,794 8,225

34,545

125,564 Corporate Laptops (CYOD)

16,450

36,104

13,901

3,979

725

Other 166

71,325 Personally Owned Mobile Devices (BYOD)

Cisco's Journey of Trusted Devices

Minimum Access Policy

Policy aligns to user demand, minimal requirements

- Encryption and Management
- Antivirus
- Device Naming
- 10 min PIN / Screenlock

Trusted Device

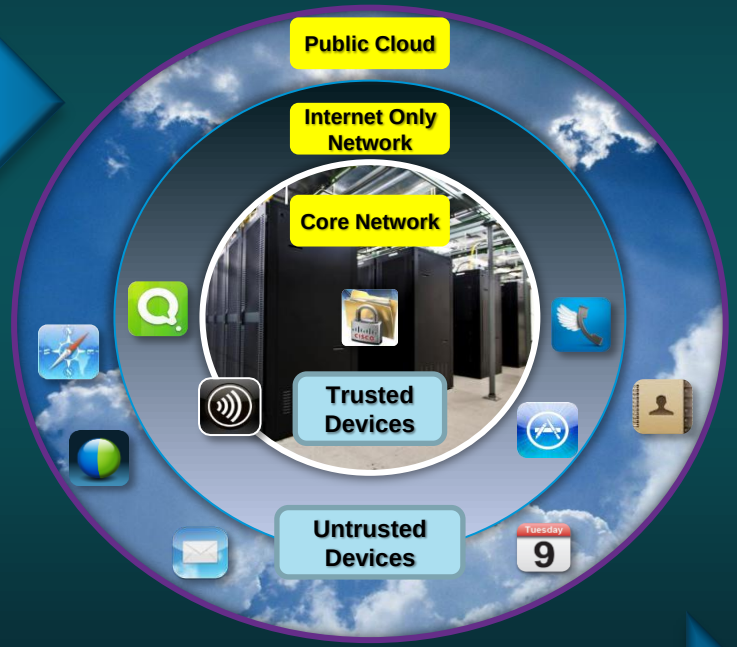
More controls needed to scale access and services

- Device Security Posture Assurance
- User authentication and authorization
- Secure storage of corporate data at rest

Coarse Differentiated Access

Differentiated Network Access

Access based on device posture leveraging Cisco TrustSec



Then → Today → Tomorrow

What is a Trusted Device?

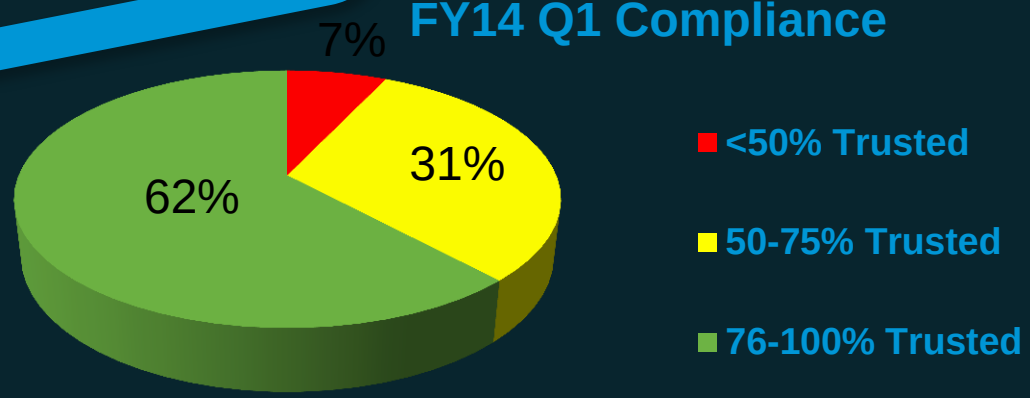
Trusted Device Elements

- Device Registration
- Anti-Malware
- Encryption (Cisco Data)
- Minimum OS
- Software Patching
- Rooted Device Detection (Mobile Devices Only)
- Remote Wipe (Cisco Data)
- Password/Screen-lock Enforcement
- Hardware/Software Inventory

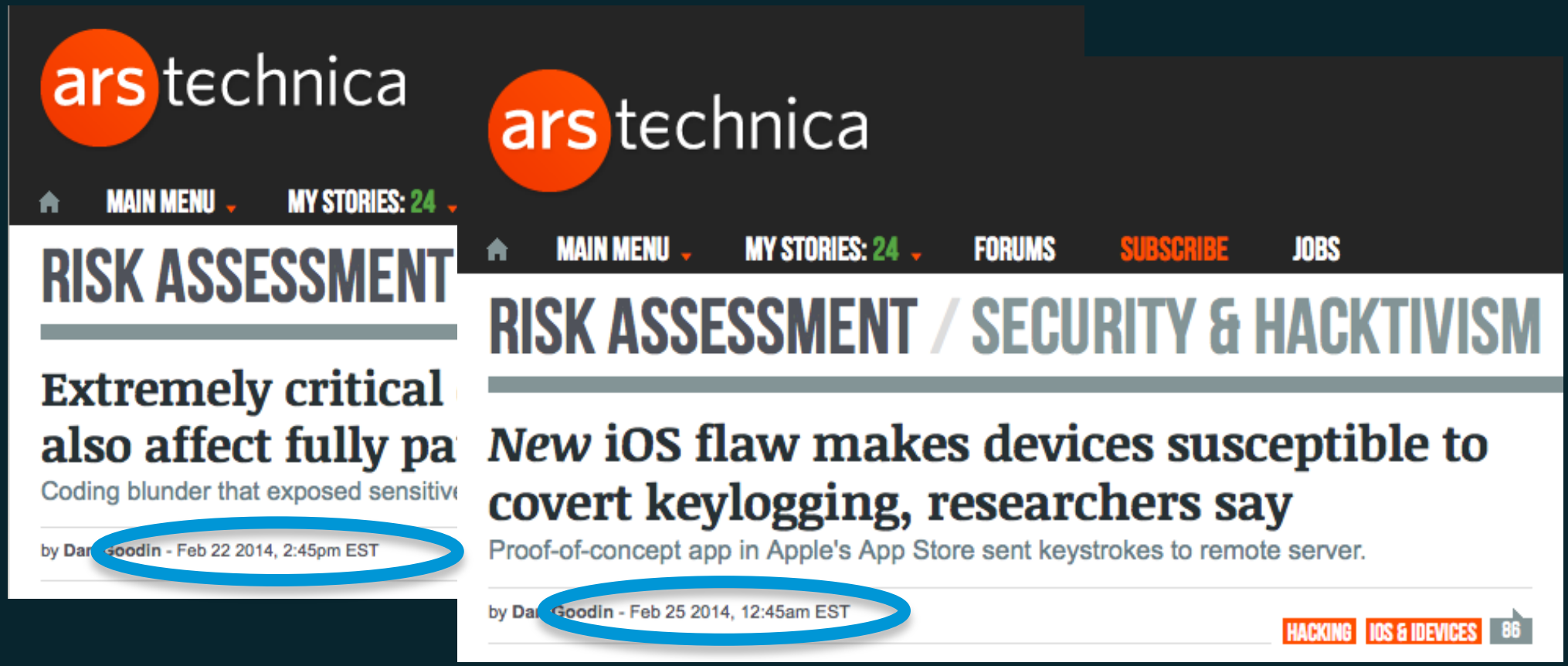
Trusted Device Solution Dashboard (FY14 Q1)

	Trusted Device Platform					
	Windows PCs	Mac PCs	Android Mobiles	iOS Mobiles	RIM Mobiles	Linux PCs (CEL)
	82,794	34,545	13,802*	52,554*	3,979	8,225*
	High	Low	High	Low	Low	Low
	88% (7/8)	88% (7/8)	33% (3/9)	66% (6/9)	100% (8/8)	63% (5/8)
		Med m	High	Med m	Low	Low

These are not the Hosts you're looking for…



Remember those hosts we're not worried about?



PLEASE GO PATCH YOUR PHONE AND YOUR MAC!

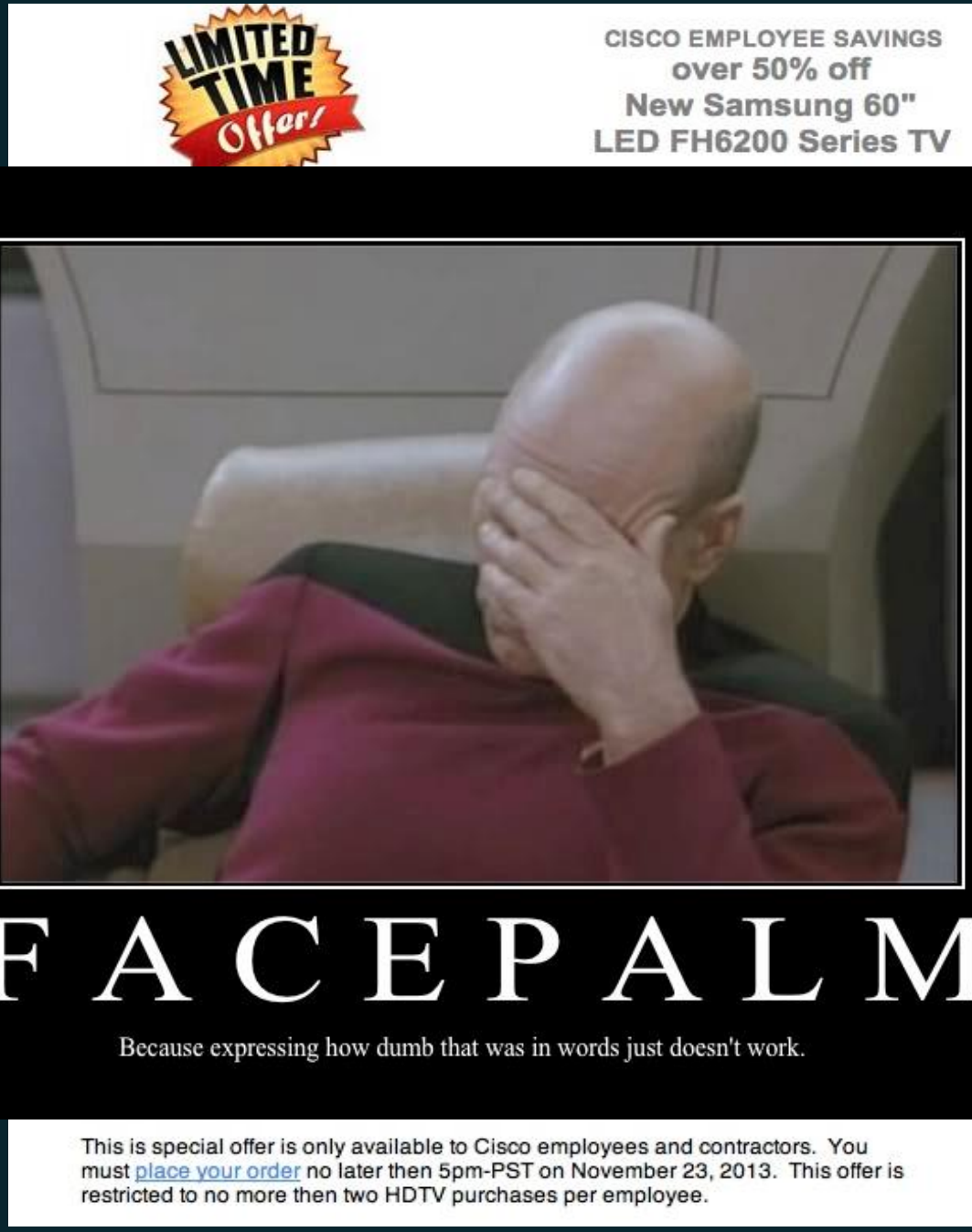
What we are faced with daily

- **Our people are faced by smart dedicated attackers**

Phishing?

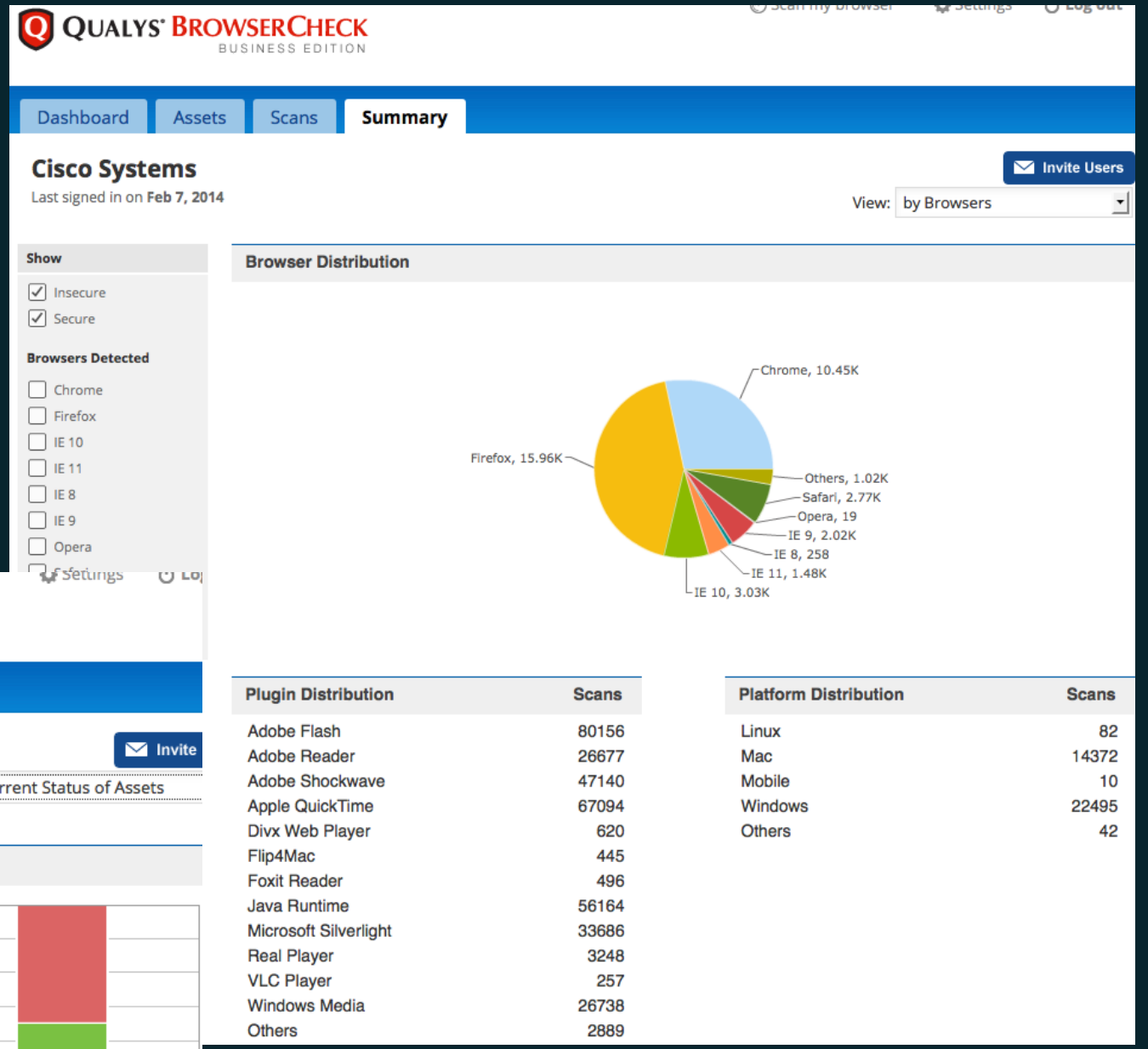
- Top Attack Vector
- We tested ~8,000 employees, and ~20% clicked the link.
- Industry averages is 30% (ouch)
- That's 1600 vectors directly against your devices!

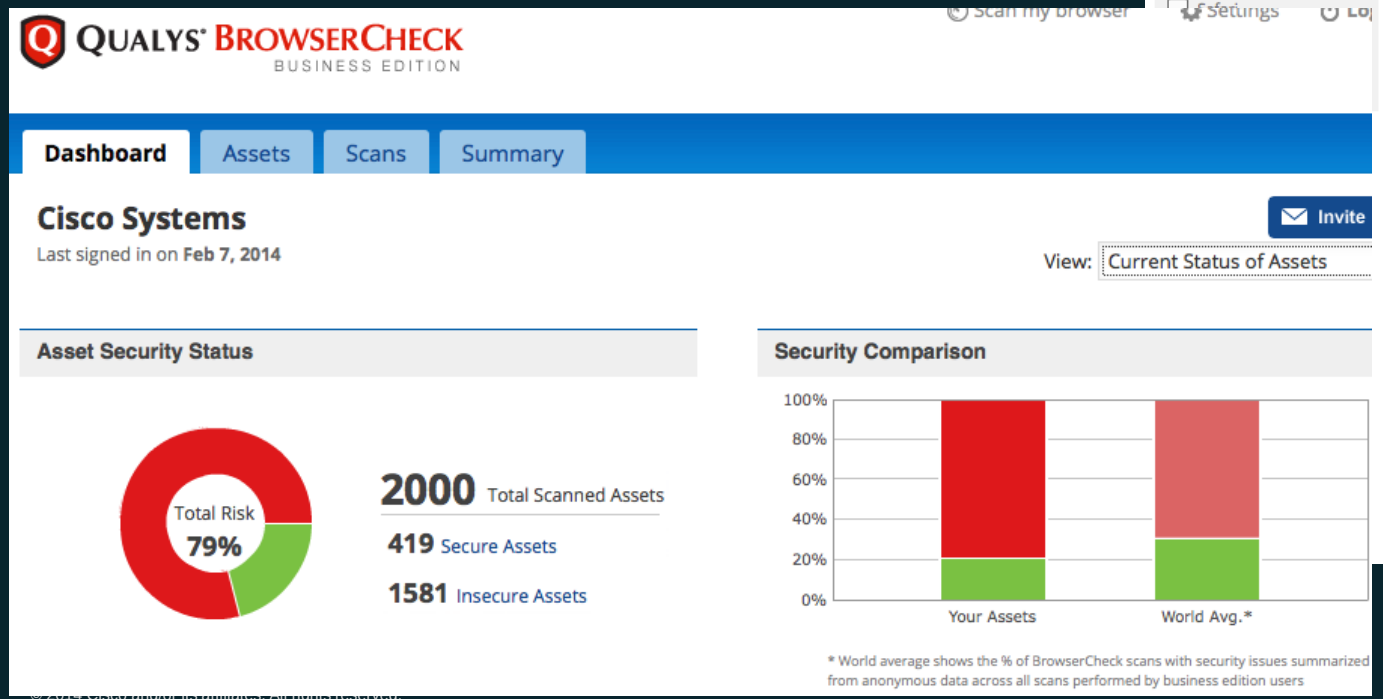
(one person thanked us for the training, then asked where they could purchase the TV…)



Getting a Handle On User Systems

- Desktop Team over tasked and under supported
- Reviewed BrowserCheck
- Currently deploying to over 100,000 systems.





Why Scan?

- Top Security Control
- Required for any conversation with an auditor

SANS

Find Training | Live Training | Online Training | Programs

Critical Security Control: 1

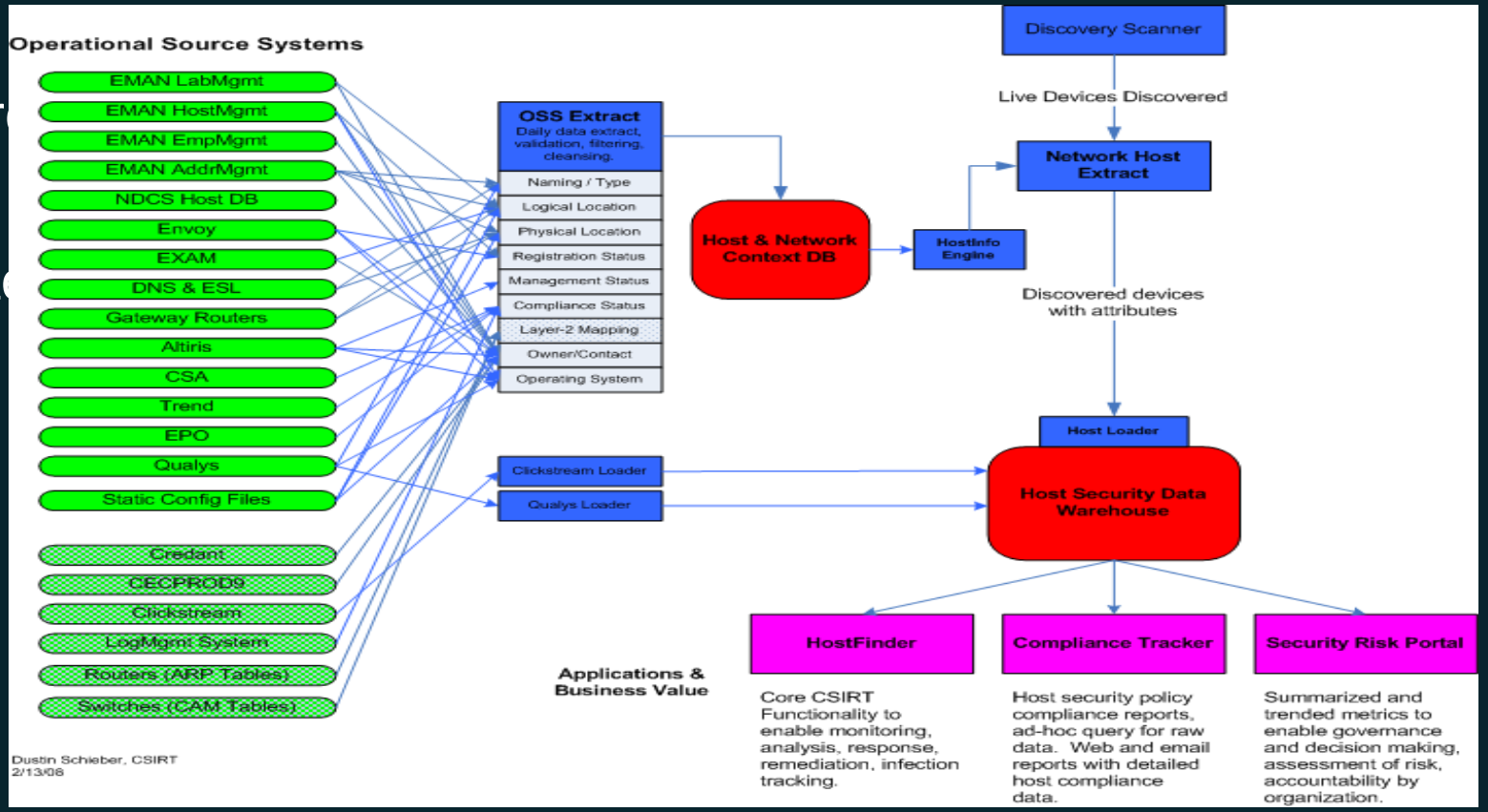
Critical Control 2 ›

ntory of Authorized and Unauthorized
ces

rocesses and tools used to track/control/prevent/correct network access by devices (computers, rk components, printers, anything with IP addresses) based on an asset inventory of which devices owed to connect to the network.

Vulnerability Management (how to run with 1.5 people)

- Internal system process pulls IP address and other information fr multiple DBs/Stores in Cisco,
- Applies business logic (associat in Japan with scanners in Asia)
- Uploads information to Qualys
- **Conducts discovery scans via half-open syn scan
- Marks ‘awake’ hosts; checks for full scan
- Collect hosts that haven’t been scanned recently – sends scan job to Qualys



Results

- Vuln data is fed to Unified Security Metrics team
- Owners are required to address issues or receive an exception

ComplianceTracker :: Action [Reporting] :: Scope [AllCisco]

This report shows the total number of vulnerable hosts by OS and logical location in the network. The count represents the number of hosts that have at least 1 confirmed vulnerability of the stated severity level.

Vulnerability Statistics - Qualys Severity 5						
	Data Center	DMZ	Lab	Partner	Desktop	TOTAL
CISCO	334	0	2800	109	1526	4660
HPUX	17	0	10	0	0	27
LINUX	1532	2	4079	179	1520	7133
OTHER	537	1	5693	594	2961	9192
SOLARIS	180	0	1448	2034	2603	4231
WINDOWS	524	0	7786	1715	8790	17100
TOTAL	3124	3	21816	4631	17400	42343

Vulnerability Statistics - Qualys Severity 4						
	Data Center	DMZ	Lab	Partner	Desktop	TOTAL
CISCO	18	0	1435	92	430	1883
HPUX	11	0	2	0	0	13
LINUX	586	3	2433	82	1344	4366
OTHER	3849	85	10376	356	4125	18435
SOLARIS	133	0	228	38	63	424
WINDOWS	158	0	1043	206	764	1965
TOTAL	4755	88	15517	774	6726	27086

Vulnerability Statistics - Qualys Severity 3						
	Data Center	DMZ	Lab	Partner	Desktop	TOTAL
CISCO	1330	18	13085	1207	42461	56897
HPUX	33	0	14	0	1	48
LINUX	22202	62	31790	1199	14355	68409
OTHER	5323	128	19510	1532	12528	37494
SOLARIS	666	1	2006	1595	2303	4976
WINDOWS	3452	9	11026	8341	59816	74303
TOTAL	33006	218	77431	13874	131464	242127

Discovery scanning in IPv6

- You can't do 'discovery' scanning – it's too big!
- Scanning a /48, with one second per IP (all ports, all protocols), will take 3.8 Billion years
- Use DHCP, DDNS, Netflow, and passive scanning to identify active hosts.
- Once ID'd, use 'dissolvable agents' to assess host posture

- IPv4 is 2^32 bits in total size (4.3 Billion total IPs)
- IPv6 is 2^128 in total size (340 Undecillion IPs)
- An IPv6 /48 has 2^80 bits (Cisco has Two)
  1,208,925,819,614,629,174,706,176 IPs (~1.2 Sextillion)
- An IPv6 /32 has 2^96 bits (Cisco has Three)
  79,228,162,514,264,337,593,543,950,336 IPs (~79 Octillion)
- An IPv6 /24 has 2^104 bits (Cisco has One)
  20,282,409,603,651,670,423,947,251,286,016 IPs (~20 Nonillion)

Summary

- It's up to you to know what's on your network – including phones/tablets
- The growth of phones and tablets is a small precursor to "The Internet of Things"
- Use tools like BrowserCheck to maintain awareness of host posture (that's how they're getting in!)
- Scanning is a vital tool in maintaining your corporate assets.